

1 **CLAIMS**

2 1. A home control system that uses electrical power lines for  
3 communications, comprising:

4 a plurality of components that are connectable for communications among  
5 themselves through the electrical power lines, said components including groups  
6 of components, wherein each group is identified collectively by a particular group  
7 identifier code;

8 components of any particular group being configured to compose and send  
9 messages that include the group identifier code of their particular group;

10 components of any particular group being further configured to receive  
11 messages from components of different groups and to disregard messages that  
12 include a group identifier code different than the group identifier code of their  
13 particular group.

14  
15 2. A system as recited in claim 1, wherein the messages do not include  
16 identifiers of specific components.

17  
18 3. A system as recited in claim 1, wherein:

19 messages composed and sent by the respective components of said  
20 particular group include first message authentication codes that are calculated  
21 using a predefined one-way function of data from the messages and of a key value  
22 that is shared between components of the particular group;

23 components of said particular group are configured to calculate a second  
24 message authentication code for each received message that is not disregarded,  
25 using the predefined one-way function of the data from the message and of the

1 shared key value, and to conclude that the received message is either not authentic  
2 or contains a data error if the first and second message authentication codes do not  
3 match.

4  
5 4. A system as recited in claim 1, wherein:

6 the components authenticate the messages using key values that are shared  
7 between components of individual groups;

8 a sending one of the components is configured to change from a current to a  
9 subsequent key value in a sequence of key values without notifying a receiving  
10 component;

11 said receiving component automatically changing from the current to the  
12 subsequent key value if the message does not authenticate with the current key  
13 value but does authenticate with the subsequent key value;

14 said receiving component concluding that the received message is either not  
15 authentic or contains a data error if the message does not authenticate with the  
16 current or the subsequent key value.

17  
18 5. A system as recited in claim 1, wherein:

19 the components authenticate the messages using key values that are shared  
20 between components of individual groups;

21 a sending one of the components is configured to change from a current to a  
22 subsequent key value in a sequence of key values without notifying a receiving  
23 component;

1       said receiving component automatically changing from the current to the  
2 subsequent key value if the message does not authenticate with the current key  
3 value but does authenticate with the subsequent key value;

4       said receiving component automatically changing from the current to a  
5 previous key value in the sequence of key values if the message does not  
6 authenticate with either the current key value or the subsequent key value, but  
7 does authenticate with the previous key value;

8       said receiving component concluding that the received message is either not  
9 authentic or contains a data error if the message does not authenticate with the  
10 previous, current, or subsequent key values.

11  
12       6.    A system as recited in claim 1, wherein the messages include data  
13 portions, and wherein different groups of the components use different formats for  
14 the data portions.

15  
16       7.    A system as recited in claim 1, wherein different groups of the  
17 components exchange data in the messages use different data exchange protocols.

18  
19       8.    A system as recited in claim 1, wherein:  
20       the messages include data portions;  
21       different groups of the components use different formats for the data  
22 portions;  
23       different groups of the components exchange data in the messages use  
24 different data exchange protocols.  
25

1           **9.**     A system as recited in claim 1, wherein:  
2           messages composed and sent by the respective components of said  
3 particular group include first message authentication codes that are calculated  
4 using a predefined one-way function of data from the messages and of a key value  
5 that is shared between components of the particular group;

6           components of said particular group are configured to calculate a second  
7 message authentication code for each received message that is not disregarded,  
8 using the predefined one-way function of the data from the message and of the  
9 shared key value, and to conclude that the received message is either not authentic  
10 or contains a data error if the first and second message authentication codes do not  
11 match;

12           the messages include data portions;

13           different groups of the components use different formats for the data  
14 portions;

15           different groups of the components exchange data in the messages use  
16 different data exchange protocols.  
17

18           **10.**    A electrical component that communicates with other electrical  
19 components of a particular component group using electrical power lines in a  
20 building, comprising:

21           a processor;

22           a transmitter that is responsive to the processor to send data using the  
23 electrical power lines;  
24  
25

1 the processor being programmed to compose and send messages in  
2 conjunction with the transmitter, each message including a group identifier code  
3 that is uniquely associated with the particular component group.  
4

5 **11.** An electrical component as recited in claim 10, wherein the  
6 messages do not include identifiers of specific electrical components.  
7

8 **12.** An electrical component as recited in claim 10, wherein messages  
9 composed and sent by the transmitter include message authentication codes that  
10 are calculated using a predefined one-way function of data from the messages and  
11 of a key value that is shared between components of the particular component  
12 group.  
13

14 **13.** An electrical component as recited in claim 10, further comprising:  
15 a receiver that functions in conjunction with the processor to receive  
16 messages from other electrical components using the electrical power lines;  
17 the processor being programmed to disregard messages that include group  
18 identifier codes different than the group identifier code of said particular  
19 component group.  
20

21 **14.** An electrical component as recited in claim 10, wherein the  
22 messages include data portions, and wherein different groups of the components  
23 use different formats for the data portions.  
24  
25

1           15.    A electrical component that communicates with other electrical  
2 components of a particular component group using electrical power lines in a  
3 building, comprising:

4           a processor;

5           a receiver that functions in conjunction with the processor to receive  
6 messages from other electrical components using the electrical power lines, such  
7 messages including different group identifier codes that are associated uniquely  
8 with respective component groups;

9           the processor being programmed to disregard messages that include group  
10 identifier codes different than the group identifier code of said particular  
11 component group.

12  
13           16.    An electrical component as recited in claim 15, wherein the  
14 messages do not include identifiers of specific electrical components.

15  
16           17.    An electrical component as recited in claim 15, wherein:

17           the messages include first message authentication codes;

18           the processor is programmed to calculate a second message authentication  
19 code for each received message that is not disregarded, based on a predefined one-  
20 way function of the data from the message and of the shared key value, and to  
21 conclude that the received message is either not authentic or contains a data error  
22 if the first and second message authentication codes do not match.

1           18.     An electrical component as recited in claim 15, the processor being  
2 programmed to perform steps comprising:

3           authenticating the messages using key values that are shared between  
4 components of respective component groups;

5           automatically changing from the current to the subsequent key value of a  
6 sequence of key values if a particular message does not authenticate with the  
7 current key value but does authenticate with the subsequent key value;

8           concluding that the received message is either not authentic or contains a  
9 data error if said particular message does not authenticate with the current or the  
10 subsequent key value.

11  
12           19.     An electrical component as recited in claim 15, the processor being  
13 programmed to perform steps comprising:

14           authenticating the messages using key values that are shared between  
15 components of respective component groups;

16           automatically changing from the current to the subsequent key value of a  
17 sequence of key values if a particular message does not authenticate with the  
18 current key value but does authenticate with the subsequent key value;

19           automatically changing from the current to a previous key value in the  
20 sequence of key values if the message does not authenticate with either the current  
21 key value or the subsequent key value, but does authenticate with the previous key  
22 value;

23           concluding that the received message is either not authentic or contains a  
24 data error if said particular message does not authenticate with the previous,  
25 current or subsequent key values.

1  
2       **20.**    An electrical component as recited in claim 15, wherein the  
3 messages include data portions, and wherein different groups of the electrical  
4 components use different formats for the data portions.  
5

6       **21.**    A method of communicating electronically between a plurality of  
7 electrical components using electrical power lines in a building, comprising the  
8 following steps:

9           designating groups of the electrical components that communicate among  
10 themselves;

11          assigning different group identifier codes to different groups of  
12 components;

13          transferring messages between components in an individual group,  
14 individual messages specifying the group identifier code of the individual group;

15          determining whether a particular message is intended for a particular  
16 component by checking whether the group identifier code of the particular  
17 message matches the group identifier code of the particular component's group.  
18

19       **22.**    A method as recited in claim 21, wherein the transferred messages  
20 do not include identifiers of specific electrical components.  
21

22       **23.**    A method as recited in claim 21, further comprising:

23          calculating first message authentication codes for the messages using a  
24 predefined one-way function of data from the messages and key values that are  
25 shared between components of individual groups;



1 including the first message authentication codes in the transferred  
2 messages;

3 calculating a second message authentication code for each message when it  
4 is received by a particular component, using the predefined one-way function of  
5 data from the message and the key value that is shared by said particular  
6 component with other components;

7 said particular component concluding that a received message is either not  
8 authentic or contains a data error if the calculated second message authentication  
9 code does not match the first message authentication code included in the  
10 message.

11  
12 **24.** A method as recited in claim 21, wherein the messages include data  
13 portions, comprising a further step of using different formats for the data portions  
14 in messages transferred between components of different groups.

15  
16 **25.** A method as recited in claim 21, comprising a further step of  
17 exchanging data in the messages using different data exchange protocols for  
18 messages transferred between components of different groups.

19  
20 **26.** A method as recited in claim 21, further comprising:  
21 authenticating the messages using key values that are shared between  
22 components of individual groups;  
23 a sending one of the components of a particular group changing from a  
24 current to a subsequent key value in a sequence of key values without notifying a  
25 receiving component of the group;

1        said receiving component automatically changing from the current to the  
2 subsequent key value if the message does not authenticate with the current key  
3 value but does authenticate with the subsequent key value.

4  
5        **27.**    A method as recited in claim 21, further comprising:

6        authenticating the messages by using a message authentication code in each  
7 message, the message authentication codes being calculated using a predefined  
8 one-way function of message data and of key values that are shared between  
9 components of individual groups;

10        a sending one of the components of a particular group changing from a  
11 current to a subsequent key value in a sequence of key values without notifying a  
12 receiving component of the group;

13        said receiving component automatically changing from the current to the  
14 subsequent key value if the message does not authenticate with the current key  
15 value but does authenticate with the subsequent key value.

16  
17        **28.**    A computer-readable storage medium having instructions that are  
18 executable by an electrical component that communicates electronically using  
19 electrical power lines in a building, the instructions being executable to perform  
20 steps comprising:

21        composing and sending data messages over the electrical power lines;

22        including a group identifier code in each message, wherein the group  
23 identifier code is uniquely associated with a particular group of components that  
24 are intended to communicate with each other.

1           29. A computer-readable storage medium as recited in claim 28,  
2 wherein the data messages do not include identifiers of specific electrical  
3 components.

4  
5           30. A computer-readable storage medium as recited in claim 28, the  
6 instructions being executable to perform further steps comprising:

7           calculating first message authentication codes for the data messages using a  
8 predefined one-way function of data from the messages and of a key value that is  
9 shared between components of said particular group;

10           including the first message authentication codes in the data messages.

11  
12           31. A computer-readable storage medium as recited in claim 28, the  
13 instructions being executable to perform further steps comprising:

14           calculating first message authentication codes for the data messages using a  
15 predefined one-way function of data from the messages and of a key values that is  
16 shared between components of said particular group;

17           including the first message authentication codes in the data messages;

18           calculating a second message authentication code for each message when it  
19 is received by a particular component, using the predefined one-way function of  
20 data from the message and the key value that is shared by the components of said  
21 particular group;

22           concluding that a message is either not authentic or contains a data error if  
23 the calculated second message authentication code does not match the first  
24 message authentication code that is included in the message.

1           **32.**    A computer-readable storage medium having instructions that are  
2 executable by a component that communicates electronically using electrical  
3 power lines in a building, the instructions being executable to perform steps  
4 comprising:

5           receiving messages from other electrical components using the electrical  
6 power lines, such messages including different group identifier codes;

7           disregarding messages that include a group identifier code different than a  
8 group identifier code is uniquely associated with a particular group of components  
9 that are intended to communicate with each other.

10  
11           **33.**    A computer-readable storage medium as recited in claim 32,  
12 wherein the messages do not include identifiers of specific electrical components.

13  
14           **34.**    A computer-readable storage medium as recited in claim 32,  
15 wherein messages composed and sent by the transmitter include first message  
16 authentication codes, the instructions being executable to perform further steps  
17 comprising:

18           calculating a second message authentication code for each received  
19 message based on a predefined one-way function of the data from the message and  
20 of a key value that is shared between components of said particular component  
21 group;

22           concluding that the message is either not authentic or contains a data error  
23 if the first and second message authentication codes do not match.

1           **35.**   A home control system that uses electrical power lines for  
2 communications, comprising:

3           a plurality of components that are connected for communications among  
4 themselves through the electrical power lines;

5           a sending one of the components being configured to send messages over  
6 the electrical power lines in accordance with steps comprising:

7                 calculating a first message authentication code based on a predefined  
8 one-way function of data from a message and of a key value that is shared  
9 between sending and receiving components;

10                including the message authentication code in the message;

11                sending the message over the electrical power lines;

12           a receiving one of the components being configured to receive messages in  
13 accordance with steps comprising:

14                 receiving a message over the electrical power lines;

15                 calculating a second message authentication code based on the  
16 predefined one-way function of the data from the message and of the a  
17 current shared key value;

18                 concluding that the message is either not authentic or contains a data  
19 error if the first and second message authentication codes do not match.  
20

21           **36.**   A home control system as recited in claim 35, wherein the shared  
22 key value is from a sequence of key values;

23           the sending component being further configured to change from a current to  
24 a subsequent key value in the sequence without notifying the receiving  
25 component;

1 the receiving component being further configured to calculate a third  
2 message authentication code based on the predefined one-way function of the data  
3 from the message and of the subsequent key value;

4 the receiving being further configured to change from the current key value  
5 to the subsequent key value if the first and second message authentication codes  
6 do not match but the first and third message authentication codes do match.

7  
8 **37.** A home control system as recited in claim 35, wherein the shared  
9 key value is from a sequence of key values;

10 the sending component being further configured to change from a current to  
11 a subsequent key value in the sequence without notifying the receiving  
12 component;

13 the receiving component being further configured to calculate a third  
14 message authentication code based on the predefined one-way function of the data  
15 from the message and of the subsequent key value;

16 the receiving being further configured to change from the current key value  
17 to the subsequent key value if the first and second message authentication codes  
18 do not match but the first and third message authentication codes do match;

19 wherein the sending and receiving components calculate the sequence of  
20 key values using a one-way function of a counter value that advances to generate  
21 each sequential key value.

1           **38.**     A home control system as recited in claim 35, wherein the shared  
2 key value is from a sequence of key values, and wherein the sending and receiving  
3 components calculate the sequence of key values using a one-way function of  
4 counter values that advance to generate each sequential key value.

5  
6           **39.**     A electrical component that is connected for communications with  
7 other electrical components of a particular group using electrical power lines in a  
8 building, comprising:

9           a processor;

10          a transmitter that is responsive to the processor to send data using the  
11 electrical power lines;

12          the processor being programmed to compose and send messages in  
13 conjunction with the transmitter, each message including a message authentication  
14 code based on a predefined one-way function of data from the message and of a  
15 key value that is shared between a plurality of components.

16  
17          **40.**     An electrical component as recited in claim 39, wherein the shared  
18 key value is from a sequence of key values, the processor being further  
19 programmed to change from a current to a subsequent key value in the sequence  
20 without notifying a receiving component.

1           **41.**     An electrical component as recited in claim 39, wherein the shared  
2 key value is from a sequence of key values, wherein the processor calculates the  
3 sequence of key values using a one-way function of a counter values that advance  
4 to generate each sequential key value.

5  
6           **42.**     A electrical component that is connected for communications with  
7 other electrical components of a particular group using electrical power lines in a  
8 building, comprising:

9           a processor;

10          a receiver that functions in conjunction with the processor to receive  
11 messages from other electrical components using the electrical power lines, such  
12 messages including first message authentication codes;

13          the processor being programmed to calculate a second message  
14 authentication code for each message based on a predefined one-way function of  
15 the data from the message and of a key value that is shared between a plurality of  
16 components;

17          the processor being further programmed to compare the first and second  
18 message authentication codes to authenticate each message.

19  
20           **43.**     An electrical component as recited in claim 42, wherein the shared  
21 key value is from a sequence of key values, the processor programmed to perform  
22 the following steps:

23          calculating a third message authentication code based on the predefined  
24 one-way function of the data from the message and of a subsequent key value in  
25 the sequence of key values;



1 further comparing the first and third message authentication codes to  
2 authenticate each message.

3 changing from the current key value to the subsequent key value if the first  
4 and second message authentication codes do not match but the first and third  
5 message authentication codes do match.

6  
7 **44.** An electrical component as recited in claim 42, wherein the shared  
8 key value is from a sequence of key values, the processor programmed to perform  
9 the following steps:

10 calculating the sequence of key values using a one-way function of a  
11 counter value that advances to generate each sequential key value;

12 calculating a third message authentication code based on the predefined  
13 one-way function of the data from the message and of a subsequent key value in  
14 the sequence of key values;

15 further comparing the first and third message authentication codes to  
16 authenticate each message.

17 changing from the current key value to the subsequent key value if the first  
18 and second message authentication codes do not match but the first and third  
19 message authentication codes do match.

20  
21 **45.** An electrical component as recited in claim 42, wherein the shared  
22 key value is from a sequence of key values, wherein the processor calculates the  
23 sequence of key values using a one-way function of a counter value that advances  
24 to generate each sequential key value.

1           **46.**    A method of communicating electronically between a plurality of  
2 electrical components using electrical power lines in a building, comprising the  
3 following steps:

4           designating groups of the electrical components that communicate among  
5 themselves;

6           sharing a key value between components of a particular group;

7           calculating a first message authentication code based on a predefined one-  
8 way function of data from a message and of the key value that is shared by  
9 components of the particular group;

10          including the message authentication code in the message;

11          sending the message over the electrical power lines;

12          receiving the message;

13          calculating a second message authentication code based on the predefined  
14 one-way function of the data from the message and of the shared key value;

15          comparing the first and second message authentication codes to  
16 authenticate each message.

17  
18           **47.**    A method as recited in claim 46, wherein the shared key value is  
19 from a sequence of key values, the method further comprising an additional step of  
20 changing from a current to a subsequent key value in the sequence without  
21 notifying receiving components.

1           **48.**    A method as recited in claim 46, wherein the shared key value is  
2 from a sequence of key values, the method further comprising:

3           calculating a third message authentication code based on the predefined  
4 one-way function of the data from the message and of a subsequent key value in  
5 the sequence of key values;

6           further comparing the first and third message authentication codes to  
7 authenticate each message.

8           changing from the current key value to the subsequent key value if the first  
9 and second message authentication codes do not match but the first and third  
10 message authentication codes do match.

11  
12           **49.**    A method as recited in claim 46, wherein the shared key value is  
13 from a sequence of key values, the method further comprising:

14           calculating the sequence of key values using a one-way function of a  
15 counter value that advances to generate each sequential key value;

16           calculating a third message authentication code based on the predefined  
17 one-way function of the data from the message and of a subsequent key value in  
18 the sequence of key values;

19           further comparing the first and third message authentication codes to  
20 authenticate each message;

21           changing from the current key value to the subsequent key value if the first  
22 and second message authentication codes do not match but the first and third  
23 message authentication codes do match.

1           **50.**     A method component as recited in claim 46, wherein the shared key  
2 value is from a sequence of key values, further comprising a step of calculating the  
3 sequence of key values using a one-way function of a counter value that advances  
4 to generate each sequential key value.

5  
6           **51.**     A method as recited in claim 46, further comprising:  
7           assigning different group identifier codes to different groups of  
8 components;  
9           specifying the group identifier code of an individual group in messages sent  
10 to components of said individual group;  
11           determining whether a particular message is intended for a particular  
12 component by checking whether the group identifier code of the particular  
13 message matches the group identifier code of the particular component's group.

14  
15           **52.**     A computer-readable storage medium having instructions that are  
16 executable by an electrical component that communicates electronically using  
17 electrical power lines in a building, the instructions being executable to perform  
18 steps comprising:

19           calculating a message authentication code based on a predefined one-way  
20 function of data from a message and of a key value that is shared by components  
21 of a particular group of electrical components;  
22           including the message authentication code in the message;  
23           sending the message over the electrical power lines.

1           **53.**    A computer-readable storage medium as recited in claim 52,  
2 wherein the shared key value is from a sequence of key values, the instructions  
3 being executable to perform further steps comprising a step of changing from a  
4 current to a subsequent key value in the sequence without notifying other  
5 components.

6  
7           **54.**    A computer-readable storage medium as recited in claim 52,  
8 wherein the shared key value is from a sequence of key values, the instructions  
9 being executable to perform a further step of calculating the sequence of key  
10 values using a one-way function of a counter value that advances to generate each  
11 sequential key value.

12  
13           **55.**    A computer-readable storage medium having instructions that are  
14 executable by an electrical component that communicates electronically using  
15 electrical power lines in a building, the instructions being executable to perform  
16 steps comprising:

17               receiving a message that contains a first message authentication code;

18               calculating a second message authentication code based on a predefined  
19 one-way function of data from the message and of a key value that is shared by a  
20 plurality of electrical components;

21               concluding that the message is either not authentic or contains a data error  
22 if the first and second message authentication codes do not match.

1       **56.**    A computer-readable storage medium as recited in claim 55,  
2 wherein the shared key value is from a sequence of key values, the instructions  
3 being executable to perform a further steps comprising:

4           calculating a third message authentication code based on the predefined  
5 one-way function of the data from the message and of a key value in the sequence  
6 of key values that is subsequent to a current key value;

7           further comparing the first and third message authentication codes to  
8 authenticate each message;

9           changing from the current key value to the subsequent key value if the first  
10 and second message authentication codes do not match but the first and third  
11 message authentication codes do match;

12  
13       **57.**    A computer-readable storage medium as recited in claim 55, the  
14 instructions being executable to perform a further step of calculating the sequence  
15 of key values using a one-way function of a counter value that advances to  
16 generate each sequential key value.